NASA Procedural Requirements

NPR 8715.3C
Effective Date: March 12, 2008
Expiration Date: March 12, 2013

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA General Safety Program Requirements

Responsible Office: Office of Safety and Mission Assurance

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | ALL |

Chapter 2. System Safety

2.1 Introduction

This chapter establishes requirements for the implementation of system safety processes to support decision making aimed at ensuring human safety, asset integrity, and mission success in programs/projects.

System safety assessment is a disciplined, systematic approach to the analysis of risks resulting from hazards that can affect humans, the environment, and mission assets. It is a critical first step in the development of risk management strategies. System safety covers the total spectrum of technical risk and management activities including safety and risk assessments and safety performance monitoring.

The format of this chapter is different than that of the rest of this NPR because of the need to discuss advanced concepts in system safety by the references.

2.2 Institutional Roles and Responsibilities

2.2.1 Mission Directorate Associate Administrators, Center Directors, program and project managers, and line managers shall ensure that system safety activities are conducted for all programs and projects including system acquisitions, in-house developments (research and technology), design, construction, fabrication and manufacture, experimentation and test, packaging and transportation, storage, checkout, launch, flight, reentry, retrieval and disassembly, maintenance and refurbishment, modification, and disposal (Requirement 25243).

2.2.2 Center Directors, through their Center SMA Directors, shall ensure that knowledgeable system safety and technical risk analysts are made available to program/project managers and Center engineering directors to define and conduct system safety activities, including assurance of prime contractor system safety activities (Requirement 25087).

2.3 System Safety Framework

2.3.1 The term "system," as used here, refers to one integrated entity that performs a specified function and includes hardware, software, human elements, and the environment within which the system operates. A "hazard," as used here, is a state or a set of conditions, internal or external to a system, that has the potential to cause harm. Generally, one or more additional conditions need to exist or additional events need to occur in conjunction with the existence of the hazard in order for an accident or mishap [1] with consequences adverse to safety [2] to result. These additional events enable the hazard to proceed to the adverse consequence. The term "mishap" is NASA's preferred generalization of an accident and it will be used in this document to refer to events leading to safety-adverse consequences. The term "accident" will be retained in the context of risk assessment methodology because of its wide acceptance in the practice of this methodology. The term "state" or "condition" is used in a broad sense to include any intrinsic property and characteristic of the material, system, or operation that could, in certain circumstances, lead to an adverse consequence . [3]

2.3.2 Hazards analysis involves the application of systematic and replicable methods to identify and understand hazards, and to characterize the risk of mishaps that involve hazards. MIL-STD-882 describes the systems engineering approach to hazard analysis. This standard is used in conjunction with the following paragraphs to develop a comprehensive scenario-based system safety analysis program.

2.3.3 Risks originate from hazards - the absence of a hazard implies a freedom from the associated risk. In the context of making decisions to manage risk, it is useful to consider "risk" as a set of triplets [4]: accident scenarios involving hazards; associated *frequencies* [5]; and associated adverse consequences. Each triplet is a statement about the likelihood of realizing a postulated accident scenario with the type and magnitude of potential adverse consequences. The expression for risk as a set of triplets is:

$$Risk = \{< accident\ scenario,\ frequency,\ consequence >\}$$

---

1 NASA defines mishap as ÒAn unplanned event that results in at least one of the following: Injury to NASA personnel, caused by NASA operations; Injury to non-NASA personnel, caused by NASA operations; Damage to public or private property (including foreign property), caused by NASA operations or NASA funded development or research projects; Occupational injury or occupational illness to NASA personnel; Destruction of, or damage to, NASA property except for a malfunction or failure of component parts that are normally subject to fair wear and tear.Ó

2 For example, the presence of fuel vapor in the crew module of a spacecraft is a hazard. Another example is the inoperability of the fire detection system.

3 For example, just having a toxic chemical in a tank constitutes a hazard because of the intrinsic toxicity property of the chemical.

4 S. Kaplan and B.J. Garrick, ÒOn the Quantitative Definition of Risk,Ó Risk Analysis, 1, 11-27, 1981.

5 The frequency estimate for each postulated accident scenario must account for the length of time during which the accident can possibly occur. This duration is often referred to as Òexposure timeÓ or Òtime at risk.Ó

The "triplet" concept of risk is operationally useful because it makes clear that in order to define, assess, and understand risk it is necessary to produce:

- A definition of the scenarios that may happen. This definition is especially useful when organized in logical fashion to identify the cause-consequence relationship of events that constitute accident scenarios.
- A characterization of the probabilities of the accident scenarios that have been identified. This characterization is expressed quantitatively in the form of a probability over some reference period of time or set of activities, or as a "frequency;" i.e., a probability per unit of time.
- A characterization of the severity of the consequences associated with the accident scenarios that have been identified. This characterization is expressed quantitatively in the form of a numeric parameter or set of parameters that best represent the magnitude and type of the adverse consequences.

It is also important to identify the uncertainties in the probabilities and consequences and to quantify them to the extent feasible.

2.3.4 NASA uses the term "safety" broadly to include human safety (public and workforce), environmental safety, and asset safety . [6] Therefore, safety-adverse consequences of interest to NASA may include:

a. General public death, injury, or illness.

b. Local public [7] death, injury, or illness.

c. Astronaut death, injury, or illness.

d. Ground crew and other workforce (occupational) death, injury, or illness.

e. Earth contamination.

f. Planetary contamination.

g. Loss of, or damage to, flight systems.

h. Loss of, or damage to, ground assets (program facilities and public properties).

---

6 The broad definition is Òfreedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.Ó In the context of risk-informed decision making, safety can be considered as an overall mission and program condition that provides sufficient assurance that accidents will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic requirements and risk criteria.

7 The term Òlocal publicÓ refers to the population in the vicinity of a site for a NASA operation but not directly associated with the operation.

2.3.5 Risk management involves making decisions that eliminate hazards or reduce the frequency and/or consequences of accidents involving hazards to an acceptable level by introducing hazard control measures and modifying system design (e.g., hardware, software) and/or procedures. Risk management may also importantly involve activities to identify and reduce uncertainties. Monitoring the effectiveness of risk reduction and uncertainty reduction strategies is an important element of risk management activities. The NASA's continuous risk management process shown below (Figure 2.1) provides an approach to track the effectiveness of implemented risk reduction strategies.

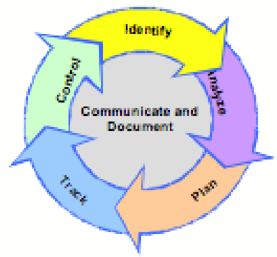

Figure 2.1: The Continuous Risk Management Process

2.3.6 Scenario-based Modeling for Hazards Analysis

2.3.6.1 Scenario-based modeling of hazards as illustrated in Figure 2.2 provides a general framework for the analysis of how hazards lead to adverse consequences. The identified scenarios then provide a basis for the assessment of risk. In the scenario modeling approach, for each hazard, an initiating event is identified, and necessary enabling conditions that result in undesired consequences are also identified. The enabling conditions often involve the failure to recognize a hazard or the failure to implement appropriate controls such as protective barriers or safety subsystems (controls). The resulting accident scenario is the sequence of events that is comprised of the initiating event and the enabling conditions and/or events that lead to the adverse consequences. Scenarios can be classified according to the type and severity of the consequences (i.e., according to their end states). In the scenario-based modeling framework, a linkage between hazards and adverse consequences of interest is established. Modeling of the characteristics of this linkage (i.e., how the presence of a hazard is linked with the occurrence of other events (e.g., hardware failures, software errors, human errors, or phenomenological events leading to formation of a mishap) should be the fabric of hazard analysis. As part of this modeling, the following items are addressed:

a. How a hazard enables or contributes to the causation of initiating events; i.e., the mechanism by which the hazard is translated to the initiating event.

b. How a hazard enables or contributes to the loss of the system's ability to compensate for (or respond to) initiating events.

c. How a hazard enables or contributes to the loss of system's ability to limit the severity of the consequences.

d. Who or what the consequences affect; i.e. the target of the consequences.

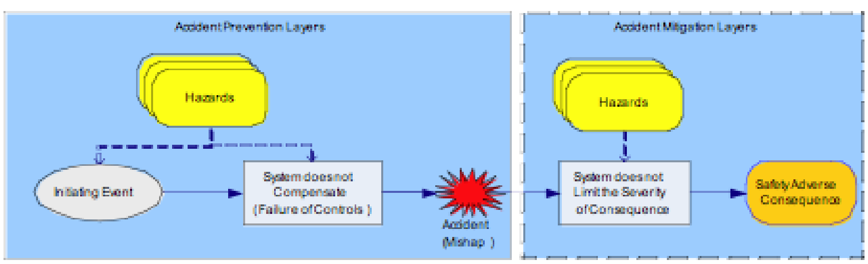

Figure 2.2: Scenario-based Modeling of Hazards

In carrying out a hazard analysis, it is important to describe the context for the hazard, which involves identifying the hazard, identifying the enabling conditions and events, and identifying the target of the consequences; i.e., does the hazard represent potential adverse consequences to humans, to the environment, or to the equipment. Analyzing hazards, in the context of the above factors, supports risk management activities that involve prevention of (reduction of frequency of) adverse accident scenarios (ones with undesired consequences) and promotion of favorable scenarios. Understanding the elements of the adverse scenarios (i.e., the structure of accident scenarios and contributing hazards), the risk significance of the adverse scenarios, and elements of successful scenarios are essential to an effective system safety and risk management program. This scenario-based risk information provides required input to risk management that is used to allocate resources optimally for risk reduction.

2.3.6.2 Evaluating uncertainties [8] is an important part of evaluating risks, in particular the uncertainties associated with the accident scenario probabilities and the accident scenario consequences. Randomness (or variability) of physical processes modeled in risk assessments requires use of probabilistic models to represent uncertainty in possible scenario outcomes. The probabilistic models for the accident scenarios reflect these process-inherent uncertainties (referred to as "aleatory uncertainties"). These process-uncertainties are realized for initiating events and system behavior and must be treated explicitly in the hazards modeling. The development of accident scenarios and their risks involves using model assumptions and model parameters that are based on what is currently known about the physics of the relevant processes and the behavior of systems under given conditions. Because there is uncertainty associated with these potentially complex conditions, probabilistic models are also used to represent the state-of-knowledge regarding the numerical parameter values and the validity of the model assumptions. These state-of-knowledge uncertainties (referred to as "epistemic uncertainties") must be properly accounted for as part of risk characterization. The expanded representation of the risk triplets that accounts for epistemic uncertainties is shown below. It is also shown notionally in Figure 2.3.

---

8 ÒUncertaintyÓ is a broad and general term used to describe an imperfect state of knowledge or a variability resulting from a variety of factors including, but not limited to, lack of knowledge, applicability of information, physical variation, randomness or stochastic behavior, indeterminacy, judgment, and approximation. Uncertainty is generally classified into two broad categories or types: epistemic uncertainty and aleatory uncertainty. Epistemic uncertainty is that uncertainty associated with incompleteness in the analystÕs (or analystsÕ) state of knowledge. Aleatory uncertainty is that uncertainty associated with variation or stochastic behavior in physical properties or physical characteristics of the system being addressed.

$$Risk = \{< accident\ scenario,\ frequency\ and\ its\ uncertainty,\ consequence\ and\ its\ uncertainty >\}$$

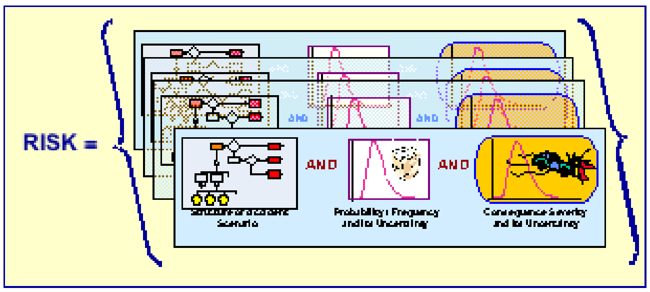

Figure 2.3: Expressing Risk as a Set of Triplets [9]

---

9 In the above, ÒRISKÓ denotes risk with uncertainty, which is an inherent part of risk.

2.3.7 Strategies to Manage Safety Risks

Risk management decisions can involve the elimination of hazards or the reduction in the probability or consequences associated with accident scenarios by modifying designs and/or introducing additional design features (e.g., hardware, software, ergonomic), and/or operational or management procedures that prevent the occurrence of an accident scenario or its propagation (individual events within the scenario) or by mitigating the consequences. Improvements in the state-of-knowledge regarding key uncertainties (i.e., uncertainty reduction) that drive the risk associated with a hazard can also be used to manage risk. (See paragraph 1.7.1 of this NPR.)

2.3.8 Program success is achieved by ensuring that technical objectives of the program are accomplished safely within the constraints of cost and schedule and consistent with stakeholder expectations. Safety is one of NASA's core values. Ensuring safety involves the following high-level safety objectives:

a. Protect public health.

b. Protect workforce health.

c. Protect the environment.

d. Protect program (systems and infrastructures needed to execute a mission) and public assets.

In order to properly support key design and operational decisions, it is necessary that design and operational alternatives [10] are analyzed not only with respect to their impact on the mission's technical and programmatic objectives, but also with respect to their impact on these high-level safety objectives. Probabilistic risk assessments [11] [11] developed as part of system safety modeling activities and supported by qualitative safety analyses (e.g., Preliminary Hazard Analysis (PHA), Fault Tree Analysis) are used to assess the impact of a decision alternative on the overall objectives. It should be noted that a typical probabilistic risk assessment model combines many engineering models including qualitative safety and reliability models (e.g., PHA, Failure Modes and Effects Analysis (FMEA)) and quantitative hardware and human reliability models for the purpose of quantifying risk. Qualitative system safety analyses are mostly "deterministic," and uncertainties which remain unquantified are managed using redundancy, design for minimum risk, physical margins, and safety factors. The roles of both probabilistic risk assessment and qualitative system safety analyses in decision making are depicted in Figure 2.4. In this NPR, the term "System Safety Models" is used to include both qualitative safety analysis and probabilistic risk assessment models. It is important to emphasize that qualitative safety analysis, to be most effective, needs to be scenario-based, even if the risks of scenarios are not explicitly quantified.

10 Decision making is the process of selecting "the most preferential (according to predetermined rules) choiceÓ from a number of available choices. Each choice represents a decision alternative.

11 Probabilistic risk assessments are used to systematically develop the set of risk triplets discussed earlier. Probabilities, magnitude of consequences, and associated uncertainties are evaluated using various analytical models (including reliability and availability models) and all available evidence, which includes physics, past experience, and expert judgment.

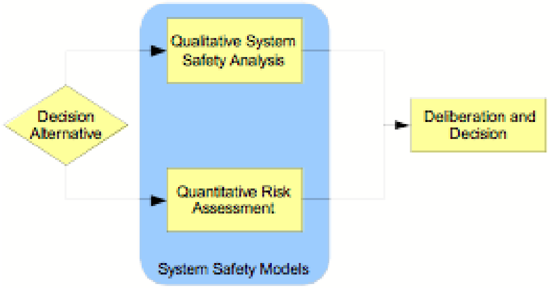

Figure 2.4: The Role of System Safety Models in Decision Making

Figure 2.4 shows importantly that probabilistic risk assessment complements and supports qualitative safety analyses and does not replace it. The deliberation that takes place before a decision is made utilizes the insights and results of both the qualitative "deterministic" analyses and the probabilistic risk assessment. Possible conflicts between these results may be resolved during the deliberation. This process of decision making is therefore risk-*informed*, not risk-*based*. It is important to note that the decision is the result of a combination of analysis and deliberation .

The deliberation at the end of the process imposes a responsibility on the decision makers who must consider subjectively the impact of each decision option on various metrics [13] that represent technical and programmatic objectives as well as on metrics that represent safety considerations. Consequently, it would be desirable to move as much of this burden as possible from the deliberation to the analysis and to begin such analysis early in Formulation. [12]

2.3.9 To facilitate the deliberation, we develop the hierarchical tree of Figure 2.5, which shows how system safety models along with other models are utilized to assess the impact of a decision alternative on safety and other objectives.

The top tier of this tree is "Program Success." The idea is to evaluate the impact on this ultimate objective of each decision alternative listed in the diamond at the bottom of the figure. Since "Program Success" is very general, a hierarchical approach is employed to develop quantitative metrics that will measure the achievement of this top-level objective. The next tier in the tree, lists the general objective categories that constitute program success; i.e., "Affordability," "Program technical objectives," "Safety," and "Stakeholder support ."[14] At the next tier, these categories are elaborated upon further by listing a number of objectives. Thus, the category "Safety" becomes the four objectives: "Protect public health," "Protect workforce health," "Protect environment," and "Protect program and public assets." The next tier of the tree, labeled "potential adverse consequences," shows quantitative metrics for each objective. For example, two metrics for the objective "protecting environment" are: "earth contamination" and "planetary contamination." These metrics, also called Performance Measures (PMs), allow quantitative assessment of the impact of each decision alternative on the objectives. This hierarchical, tree-like structure shows the objectives that the decision maker values in making the decision. It provides a convenient structure for:

a. Identification of safety PMs (measures of safety adverse consequences) and other technical and programmatic PMs in the context of the program's high-level objectives.

b. Formulating risk tradeoff studies.

c. Capturing of decision maker's preferences [15] .

d. Ranking of decision alternatives according to their desirability (based on consideration of PMs and preferences).

e. Deliberation that is required as part of the decision-making process.

12 Details on the analytic-deliberative decision-making process are given in the National Research CouncilÕs report ÒUnderstanding Risk: Informing Decisions in a Democratic Society,Ó National Academy Press, Washington, DC, 1996.

13 The Institute of Electrical and Electronics Engineers (IEEE) defines metric as a quantitative measure of the degree to which a system, component, or process possesses a given attribute.

14 These objectives must be fundamental objectives; i.e., objectives that the decision maker fundamentally cares

about.

15 The PMs (adverse consequences), in general, are not valued equally by the decision maker.

2.3.10 A PM is a metric that is related to risk and/or the constituents of risk (e.g., probability, consequence). It provides risk insight into a process, a project, or a product to enable assessment and improvement. Safety PMs are metrics that provide measures of the safety performance of a system. Because adverse space mission mishaps are rare and an absence of mishaps does not assure that no mishaps will occur in the future, safety PMs provide a means of assessing and monitoring safety performance to enable design and operational decisions aimed at preventing mishaps and optimizing safety. High level safety PMs (see the hierarchy shown in Figure 2.5) can be defined in terms of the probability of a consequence type of a specific magnitude (e.g., probability of any general public deaths or injuries) or the expected magnitude of a consequence type (e.g., the number of public deaths or injuries). Metrics such as "Probability of failure to meet a mission critical function" can be used as non-safety PMs. Safety and non-safety PMs, along with other performance measures such as reliability, provide decision makers with the ability (1) to set performance goals (e.g., safety goals), (2) to trade performances, and (3) to monitor performances at different stages of the system life cycle.

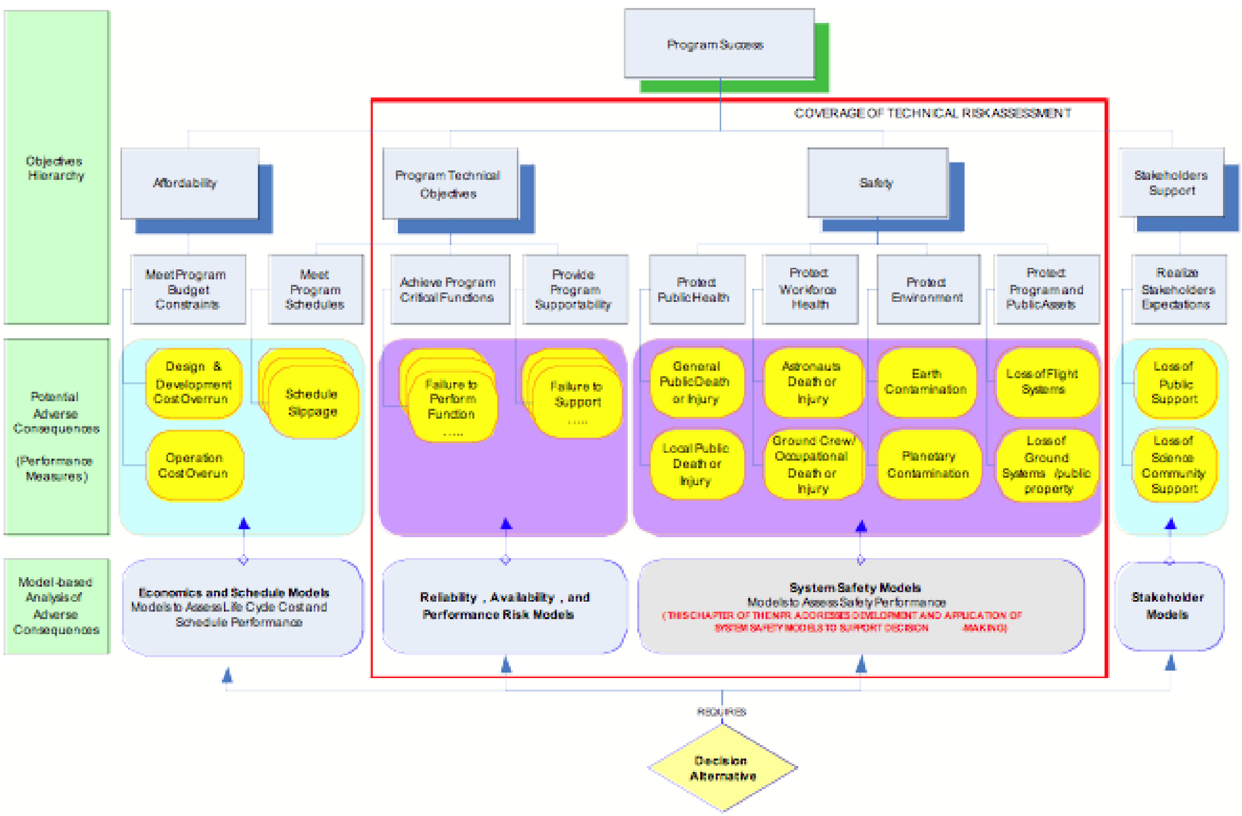

Figure 2.5: The Role of System Safety Models and Other Models in Risk-informed Decision Making

2.3.11 Relationship of System Safety Technical Processes with Other Technical Processes

The system safety technical processes provided in this chapter cannot be effective unless they are performed by well-trained and experienced safety analysts and are supported by engineering and safety-related activities that include:

a. Ensuring that safety, software, and quality standards are applied and utilized throughout the project life cycle (e.g., NASA-STD-8719.13, Software Safety Standard, and NASA-STD-8739.8, Software Assurance Standard). These are included in the box "Qualitative System Safety Analysis" of Figure 2.4 and in the deliberation.

b. Monitoring processes to ensure that lessons learned are used as feedback to inform safety-related models and activities.

c. Ensuring that best practices in system engineering are followed in the design of the system.

Note: Requirements for system engineering are provided in NPR 7123.1, Systems Engineering Procedural Requirements.

2.4 Scope of System Safety Modeling

Decision makers throughout the entire life cycle of the project, beginning with concept design and concluding with decommissioning, must consider safety. However, the level of formality and rigor that is involved in implementing the system safety processes should match project potential consequences, life cycle phase, life cycle cost, and strategic importance. To assist in determining the scope of activities for safety evaluations as a function of project characteristics, two tables are provided. The categorization scheme identified in Table 2.1 is used to determine a project priority. This table is similar to Table 1 from NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects.

Table 2.1. Criteria for Determining the Project Priority

<table>
<tr><th>CONSEQUENCE CATEGORY</th><th colspan="2">CRITERIA / SPECIFICS</th><th>Project Priority Ranking</th></tr>
<tr><td rowspan="4">Human Safety and Health</td><td rowspan="3">Public Safety and Health</td><td>Planetary Protection Program Requirement</td><td rowspan="7">I</td></tr>
<tr><td>White House Approval (PD/NSC-25)</td></tr>
<tr><td>Space Missions with Flight Termination Systems</td></tr>
<tr><td colspan="2">Human Space Flight</td></tr>
<tr><td rowspan="5">Mission Success (for non-human rated missions)</td><td colspan="2">High Strategic Importance Projects</td></tr>
<tr><td colspan="2">Limited Window</td></tr>
<tr><td colspan="2">High Cost (See NPR 7120.5)</td></tr>
<tr><td colspan="2">Medium Cost (See NPR 7120.5)</td><td>II</td></tr>
<tr><td colspan="2">Low Cost (See NPR 7120.5)</td><td>III</td></tr>
</table>

Once the project priority is determined, the scope of system safety modeling is determined using Table 2.2.

2.4.2 Projects identified as "Priority I" ranking from Tables 2.1 are generally the most visible and complex of NASA's product lines. Because of this, the system safety technical processes for Priority I projects must include probabilistic risk assessment as specified in NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects. For Priority II or III projects, Table 2.2 provides latitude to adjust the scope of system safety modeling. This graded approach to the application of system safety modeling also operates on another dimension. That is, the level of rigor and detail associated with system safety modeling activities must be commensurate with the availability of design and operational information . [16] The two-dimensional nature of the graded approach is intended to ensure that allocation of resources to system safety technical activities considers the visibility and complexity of the project and to ensure that the level of rigor associated with system safety models follows the level of maturity of the system design.

---

[16] For example, during the formulation phase, an order-of-magnitude or bounding assessment may be performed. In this type of assessment, the probability and/or the magnitude of consequence is approximated or bounded instead of deriving a best-estimate. These assessments are useful for screening purposes and initial risk tradeoff studies.

Table 2.2: Graded Approach to System Safety Modeling

Priority Ranking	Scope (The level of rigor and details are commensurate with the level of design maturity)

I	Probabilistic risk assessment (per NPR 8705.5) supported by qualitative system safety analysis
II	Qualitative system safety analysis supplemented by probabilistic risk assessment where appropriate
III	Qualitative system safety analysis

2.5 Core Requirements for System Safety Processes

The system safety modeling approaches previously described should be implemented as part of technical processes that represent system safety activities. Conceptually, system safety activities consist of three major technical processes as shown in the circular flow diagram in Figure 2.6. These processes are designed to systematically and objectively analyze hazards and identify the mechanism for their elimination or control. These processes begin in the conceptual phase and extend throughout the life cycle of a system including disposal. In general, requirements for safety system technical processes must provide a risk-informed perspective to decision makers participating in the project life cycle. The three critical technical processes to a successful system safety program are (1) system safety modeling, (2) life cycle applications of models for risk-informed decisions and, (3) monitoring safety performance. The circular flow indicates that these technical processes are linked and are performed throughout the project life cycle. A System Safety Technical Plan is used to guide the technical processes and establish roles and responsibilities. This plan is established early in the formulation phase of each project and updated throughout the project life cycle.

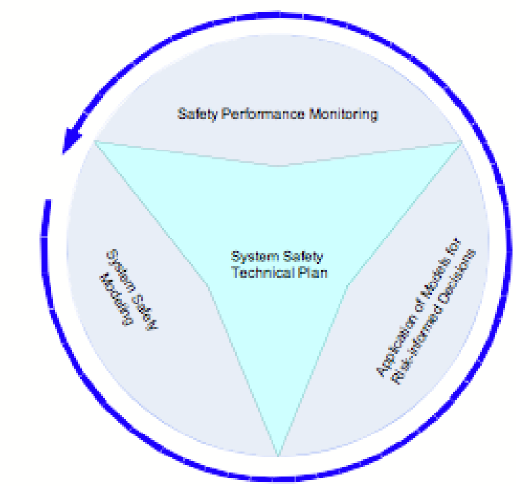

Figure 2.6: The System Safety Technical Processes

2.5.1 System Safety Technical Plan (SSTP)

The SSTP is designed to be a technical planning guide for the technical performance and management of the system safety activities. The SSTP can be a stand-alone document, or part of the SMA plan or the Systems Engineering Management Plan (SEMP). It provides the specifics of the system safety modeling activities and describes what and how safety adverse consequences will be modeled, how system safety models (qualitative and probabilistic risk assessments) will be integrated and applied for risk-informed decision making and safety monitoring, how the technical team(s) responsible for generating and maintaining system safety models will interact with the system engineering organizations, the reporting protocol, and the cost and schedule associated with accomplishing system safety modeling activities in relation to the critical or key events during all phases of the life cycle.

2.5.1.1 Project managers shall:

a. Ensure, for Category I project/programs, that the SSTP is approved by the governing Program Management Council (PMC) and has concurrence by the cognizant SMA managers and the project's senior engineer (Requirement).

b. Ensure that the System Safety Manager and the prime contractor (for out-of-house projects) have the resources to implement the SSTP (Requirement 25082).

c. Ensure, for Category I project/programs, that changes to the SSTP are approved by the governing PMC and have concurrence by the Chief, Safety and Mission Assurance (Requirement).

d. When the SSTP is not an integral part of the SEMP, ensure the SSTP is coordinated with the SEMP for the integration of system safety activities with other system engineering technical processes (Requirement).

2.5.1.2 The Center SMA Director shall:

a. In coordination with the program/project manager, assign a System Safety Manager to have specific responsibility for the development and implementation of the SSTP (Requirement 25081).

b. Ensure that the assigned System Safety Manager has demonstrated expertise in safety analysis including, in the case of Category I and II projects, the application of probabilistic risk assessment techniques (Requirement).

c. Ensure that all personnel with project safety oversight responsibilities are funded by other than direct project funding sources (Requirement).

2.5.1.3 The assigned System Safety Manager shall:

a. Develop a SSTP during the project formulation phase and update the plan throughout the system life cycle (Requirement).

b. Ensure that the scope of system safety technical processes in the SSTP follows the graded approach specified in Tables 2.1 and 2.2 (Requirement 32105).

c. Ensure that the SSTP provides the specifics of the system safety modeling activities and their application to risk-informed decision making and safety monitoring throughout the project life cycle (Requirement).

d. In consultation with the project managers, establish and document in the SSTP the objectives and scope of the system safety tasks and define applicable safety deliverables and performance measures (Requirement).

e. Provide technical direction and manage implementation of system safety activities as specified in the SSTP (Requirement).

f. Ensure that system safety engineering activities are integrated into system engineering technical processes (Requirement).

g. Determine the acceptability of residual risk stemming from safety assessments (Requirement).

h. Ensure that specific safety requirements are integrated into overall programmatic requirements and are reflected in applicable program and planning documents including the statement of work for contractor designs (Requirement 32120).

i. Maintain appropriate safety participation in the program design, tests, operations, failures and mishaps, and contractor system safety activities at a level consistent with mishap potential for the life of the program (Requirement 25094).

j. Establish an independent safety reporting channel to keep the Center SMA Director apprised of the system safety status (including tests and operations), particularly regarding problem areas that may require assistance from the Center, the NASA Engineering and Safety Center, or Headquarters (Requirement 25095).

k. Support OSMA requirements for audits, assessments, and reviews (Requirement).

2.5.2 System Safety Modeling

Developing and maintaining technically sound and tractable safety models are essential activities for ensuring safety. In these activities, analysts use all the relevant and available information including design documents, operational procedures, test results, operational history, and human and software performance to develop comprehensive system safety models. Developing these models is multidisciplinary and may involve diverse and geographically dispersed groups. Thus, it is important for the safety modeling activities to be coordinated in order to ensure consistency and technical quality.

Safety models need to be synchronized with the system design and operational state-of-knowledge to ensure the models match the collected engineering information during operation with model predictions.

2.5.2.1 System Safety Managers shall ensure that the system safety modeling activities are fully integrated into system engineering and are supported by domain, systems, and specialty engineers (Requirement).

2.5.2.2 System engineers shall:

a. Ensure that system safety models use systematic, replicable, and scenario-based techniques to identify hazards, to characterize the risk of accidents, to identify risk control measures, and to identify key uncertainties (Requirement 32122).

b. Initially conduct system safety analyses during project formulation and design concept phases (prior to the Preliminary Design Review) and maintain and update these analyses continuously throughout the project life cycle (Requirement 32126).

c. Ensure, for Category I and II program/projects, probabilistic risk assessment techniques are used for system safety analysis (Requirement).

d. Ensure that the system safety models are developed in an iterative process to allow model expansion, model updating, and model integration as the design evolves and operational experience is acquired (Requirement).

> **Note: Relevant leading-indicator (or precursor [17]) events should be documented and evaluated for their impact on the system safety analyses assumptions. Trending of these precursor events should be conducted and contrasted to applicable PMs.**

e. Use system specific and all relevant data including failure histories, mishap investigation findings, and the NASA LLIS in system safety analysis (Requirement).

f. Maintain an up-to-date database of identified hazards, accident scenarios, probabilities and consequences, and key uncertainties throughout the life of the program (Requirement 25093).

g. Document the bases for the system safety analyses including key assumptions, accident scenarios, probabilities, consequence severities, and uncertainties such that they are traceable (Requirement).

2.5.3 Application of System Safety Models for Risk-informed Decisions

Safety and technical risk considerations are critical in the decision-making process. When faced with a decision, several conflicting alternatives may be available to the decision maker. In a risk-informed decision-making framework, the decision maker considers safety and other technical attributes as well as programmatic attributes, such as cost and schedule, to select the best decision alternative.

2.5.3.1 Program/project managers shall:

a. Ensure that a framework is constructed for systematically incorporating system safety analysis results into the evaluation of decision alternatives (Requirement).

b. Establish and document a formal and transparent decision-making process for hazard closure [18] and formally accepting residual risk that has been determined to be acceptable by the cognizant technical authority (Requirement 25085).

c. Ensure acceptable residual risks [19] are accepted in writing (Requirement 32114). (See paragraph 1.6 of this NPR.)

d. Ensure that decisions to accept risk are coordinated with the governing SMA organization and communicated to the next higher level of management for review (Requirement 32115). (See paragraph 1.6.2 of this NPR.)

e. Where residual risks have been determined by either the cognizant technical authority or the cognizant SMA authority as "unacceptable," initiate risk mitigation/control activities, as appropriate, to reduce the risk to an acceptable level (Requirement).

f. Ensure that the requirements of this Chapter are specified in related contracts, memoranda of understanding, and other agreement documents (Requirement). (See Chapter 9 of this NPR.)

---

17 A precursor is an occurrence of one or more events that have significant failure or risk implications.

18 Closure of a hazard condition or other safety issue is the demonstration that all safety requirements expressly formulated to address the condition or issue have been satisfied.

19 Residual risk is the level of risk that remains present after applicable safety-related requirements have been satisfied. In a risk-informed context, such requirements may include measures and provisions intended to reduce risk from above to below a defined acceptable level.

2.5.3.2 The System Safety Manager shall:

a. Ensure that system safety models are constructed to support the implementation of the risk-informed decision framework (Requirement).

b. Ensure that the system safety models incorporate all the safety attributes important to risk-informed decision making by working with the project manager and other decision makers as deemed appropriate (Requirement).

c. Establish the methods and tools that are used in the risk-informed framework (Requirement).

d. Check and validate the methods and tools before implementation and obtain concurrence from the project manager (Requirement).

e. Document the bases for the methods and tools used and analytical results (Requirement).

2.5.4 Performance Monitoring

Safety, like other performance attributes, is monitored during the entire life cycle to ensure that an acceptable level of safety is maintained.

2.5.4.1 Project managers shall ensure that the performance attributes and precursors that are identified as being important indicators of system safety are monitored (Requirement).

2.5.4.2 The System Safety Manager shall:

a. Establish the methods and tools that are used in the performance monitoring and precursor assessments (Requirement).

b. Check and validate the methods and tools used for performance monitoring and precursor assessments before implementation (Requirement).

c. Maintain an up-to-date database of the performance monitoring results and precursor results (Requirement).

d. Ensure that the performance monitoring and precursor data are fed back into system safety analyses and the results updated (Requirement).

e. Document the bases for the methods and tools that are used in the performance monitoring and precursor assessments (Requirement).

2.6 System Safety Reviews

System Safety and Mission Success Program Reviews are conducted in conjunction with other program milestones. The purpose of these reviews is to evaluate the status of system safety and risk analyses, risk management, verification techniques, technical safety requirements, and program implementation throughout all the phases of the system life cycle.

2.6.1 The program/project manager shall:

a. Conduct periodic system safety and mission success reviews of their program/project depending on the complexity of the system (Requirement 25099).

> *Note: The greater the risks, complexity of the system, or visibility of the programs, the greater the independence and formality of the reviews.*

b. Document the periodicity of the System Safety and Mission Success Program Reviews in the SSTP (Requirement).

c. Ensure that the System Safety and Mission Success Program Reviews focus on the evaluation of management and technical documentation, hazard closure, and the safety residual risks remaining in the program at that stage of development (Requirement 32129).

d. Establish and maintain dedicated independent assessment activities for Priority I programs and projects, such as the Constellation Program (Requirement 32113).

2.6.2 The System Safety Manager shall:

a. Conduct periodic independent reviews of the system safety tasks keyed to project milestones (Requirement 25091).

b. Assist and support independent review groups established to provide independent assessments of the program (Requirement 25092).

c. Support the OSMA independent safety assessment process to determine readiness to conduct tests and operations having significant levels of safety risks (Requirement).

2.7 Change Review

Systems are changed during their life cycle to enhance capabilities, improve safety, provide more efficient operation, and incorporate new technology. With each change, the original safety aspects of the system can be impacted, either increasing or reducing the risk. Any aspect of controlling hazards can be weakened, risks can be increased, or conversely, risks can be decreased. Even a change that appears inconsequential could have significant impact on the baseline risk of the system. Accordingly, proposed system changes should be subjected to a safety review or analysis, as appropriate, to assess the safety and risk impacts, including implications on controls and mitigations for significant hazards and FMEA/CILS.

2.7.1 The project manager and the System Safety Manager shall:

a. Update the system safety analyses to identify any change in risk (Requirement 25102).

b. Ensure that safety personnel assess the potential safety impact of the proposed change and any changes to the baseline risk and previously closed hazards (Requirement 32137).

c. Ensure that proposed changes to correct a safety problem are analyzed to determine the amount of safety improvement (or detriment) that would result from incorporation of the change (Requirement 32138).

d. Ensure that the safety impact for every change that is proposed to a program baseline (even if the statement is "No Impact") is documented (Requirement 32139).

2.8 Documentation

The maintenance of the SSTP is required to provide ready traceability from the baseline safety requirements, criteria, and efforts planned in the conceptual phases through the life cycle of the program.

2.8.1 The project manager (or designated agent) and the System Safety Manager shall:

a. Ensure that all pertinent details of the system safety analysis and review are traceable from the initial identification of the risks through their resolution and any updates in the SSTP (Requirement 25100).

b. Ensure that records are maintained per NPR1441.1, NASA Records Retention Schedules (Requirement 32130).

2.8.2 The System Safety Manager shall:

a. Submit a system safety analysis report to the program/project manager at each milestone (formulation, evaluation, implementation, or other equivalent milestones [e.g., Safety Requirements Review [20], Preliminary Design Review, Critical Design Review, and Flight Readiness Review]) detailing the results of the system safety analyses completed to date to document the status of system safety tasks (Requirement 25101).

b. Ensure that each submitted revision to the system safety analysis report lists the risks that have been addressed, the risks that have yet to be addressed, and expected residual risks that will remain following the implementation of risk reduction strategies (Requirement 32132).

c. Ensure that the system safety analysis report documents management and technical changes that affect the established safety baseline (by changes in the planned approach, design, requirements, and implementation) and is revised when required (Requirement 32133).

d. Ensure that a final approved system safety analysis report is produced that contains a verification of the resolution of the risks and a written acceptance of the residual risks from the program/project manager to complete the audit trail (Requirement 32134).

---

20 Safety requirements include both deterministic and risk-informed requirements. A deterministic safety requirement is the qualitative or quantitative definition of a threshold of action or performance that must be met by a mission-related design item, system, or activity in order for that item, system, or activity to be acceptably safe. A risk-informed requirement is a safety requirement that has been established, at least in part, on the basis of the consideration of a safety-related risk metric and its associated uncertainty.

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS